

Appl. No. 09/390,362
Reply to Office Action of: April 26, 2006

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key α and a public key derived from the private key α , said public key being [[and]] available to the other of said pair of correspondents, said method comprising the steps of:

subdividing said plaintext message into a first plaintext bit string H and a second plaintext bit string V;

utilizing computing a first signature component c as a function of said first plaintext bitstring bit string H to compute a first signature component c, in which the wherein the plaintext bit string H is hidden in said signature component c;

forming from computing an intermediate signature component c' as a function of said first signature component c and said second plaintext bit string V, an intermediate signature component c';

utilizing computing a second signature component s as a function of said intermediate signature component c' and said private key α to provide a second signature component s, in which the plaintext is hidden; and

forming a signature (s, c, V) by including containing said first signature component c, said second signature component s, and said second plaintext bit string V as discrete signature components;

whereby during verification, said second plaintext bit string V is available from said signature (s, c, V) as an input to a verification protocol.

2. (previously presented) A method according to claim 1 wherein redundancy in said first plaintext bit string H is compared to a predetermined level prior to computing said first signature component c.

3. (previously presented) A method according to claim 2 wherein said redundancy is adjusted to

Appl. No. 09/390,362
Reply to Office Action of: April 26, 2006

exceed a predetermined level.

4. (previously presented) A method according to claim 3 wherein data is added to said first plaintext bit string H to adjust said redundancy.
5. (previously presented) A method according to claim 4 wherein an indicator is included in said first plaintext bit string H to indicate additional data.
6. (previously presented) A method according to claim 1 wherein said second signature component s is generated by hashing said first signature component c and said second plaintext bit string V.
7. (currently amended) A method of verifying a plaintext message from a signature of a purported signer in a data transmission system, said plaintext message being subdivided into a first plaintext bit string H and a second plaintext bit string V, said signature formed as a set of discrete components, said components including signature containing at least one a first component having only computed as a function of said first plaintext bit string H whereby said bit string H is encrypted therein, and a second component being said second plaintext bit string V as a second component, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said method comprising the steps of:
 - generating a value by combining said [[one]] first component with said second plaintext bit string V;
 - recovering said first plaintext bit string H from said combination value using publicly available information of the purported signer including said public key; [[and]]
 - examining said recovered first plaintext bit string H for a predetermined characteristic[[.]]; and
 - verifying said message if said predetermined characteristic is present.

8. (currently amended) A method according to claim 7 wherein said combination of said [[one]] first component and said second plaintext bit string V includes hashing a combination of said

Appl. No. 09/390,362
Reply to Office Action of. April 26, 2006

[[one]] first component and said second plaintext bit string V.

9. (previously presented) A method according to claim 7 wherein said predetermined characteristic is the redundancy of said recovered first plaintext bit string H.

10. (currently amended) A method according to claim 9 wherein said signature includes a third component derived from a combination of said [[one]] first component and said second plaintext bit string V and said first plaintext bit string H is recovered utilising said third component.

11. (currently amended) A method according to claim 1 wherein said first signature component *c* is formed computed by applying a function to said first plaintext bit string H and said first plaintext bit string H may be recovered from said first signature component *c* by applying a complementary function to said first signature component *c*.

12. (currently amended) A method according to claim 11 wherein said function is encryption with an encryption key, a decryption [[said]] key is recoverable computable from information available in said signature, and said complementary function is decryption with said decryption key.

13. (currently amended) A method according to claim 12, wherein said encryption key is a short-term public key derived from a ~~short term~~ private key random integer used in the provision of said second signature component.